UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/605,173	09/12/2003	ASHOT ANDREASYAN	PR 1803.01 US	2172

31883 7590 09/30/2008

DVA/PIONEER RESEARCH CENTER USA, INC.
2265 E. 220TH STREET
LONG BEACH, CA 90810

EXAMINER	
TRUVAN, LEYNNA THANH	
ART UNIT	**PAPER NUMBER**
2135	
MAIL DATE	**DELIVERY MODE**
09/30/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/605,173	ANDREASYAN, ASHOT	
	Examiner	Art Unit	
	Leynna T. Truvan	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 June 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-35* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-35 remains pending.

Response to Arguments

2. Applicant's arguments filed 6/20/1008 have been fully considered but they are not persuasive.

The 101 rejection of claims 1-32 are withdrawn.

Examiner traverses argument on pg.14 with regard to the prior art, Qu, disclosing an ID-based certificate generation process which is not the same as the claimed invention that uses certificate parameters for a key exchange. The claimed broadly limits the certificate parameters being digital signature standard parameters which may be variety of different types of data/information (i.e signature, hash, key, cryptographic algorithm, etc.) involved that constitutes digital signature parameters (col.9, lines 20-50). The ID-based certificate generation process was explained as the background of Qu's invention but improves on this process by multiple exponentiations. Plus, being ID-based is not relevant to applicant's invention since it is not claimed and that Qu reads on the claim invention of 3 exponentiations as claimed.

Examiner traverses argument on pg.14: with regard to Qu requires 4 exponentiation rather than the claim invention's 3 exponentiation because Qu clearly suggests 3 exponentiation operations (col.20, lines 1-7 and 40-42). Qu discloses various schemes for key generation and certificate computation where one of schemes is the three exponentiation operations to get shared key.

Examiner traverses argument on pg.15: that the present invention does not generate public key certificates and that the public key is used for key exchange only. Since applicant did not specify the claim that is referring to for the arguments, examiner will choose claim 1 when referring to claim

limitations or language. Claim 1 (line 5) clearly recites performing a first exponentiation operation to generate a first public key. Examiner is unclear whether the claimed "generate a first public key" is not related to a public key certificate or if applicant meant for the claimed invention to be different than that of the public key certificates. Whatever the case may be, Qu reads on the claimed performing a first exponentiation operation to generate a first public key performing a first exponentiation operation to generate a first public key **(col.2, lines 38-47 and col.3, lines 57-67).**

Examiner traverses argument on pg.15: that the operations in the claimed invention are done by peers and not by CA. However, the limitations of performing 2nd exponentiation and third exponentiation does not specify whether the peer(s) or the CA performing these operations. Since applicant did not specify the claim that is referring to for the arguments, examiner will choose claim 1 when referring to claim limitations or language. For instance, claim 1 recites "performing a second exponentiation operation to generate a first shared secret key for the second peer using at least one parameter from the plurality of first parameters" and "performing a third exponentiation operation to generate a second shared secret key for the first peer using the first public key from the second peer and a private key from the first peer. This merely specifies using certain keys from a particular peer to generate for a particular peer but does not specify exactly who is performing these operations. Therefore, whether one of the peers or the CA performs some of the limitations is irrelevant and inconsistent with what is claimed because the invention fails to claim otherwise.

Examiner traverses argument on pg.16: Lenstra is combined with Qu to further disclose the advantage of the three exponentiation operations. Lenstra discloses the use Algorithm 2.4.4 with n=z and B replaced by xtr(u.sub.1) to compute .kappa.=xtr((g.sub.1).sup.zr). 8. As in [8: Section 5.2], compute the decryption key K by hashing .kappa. to an l-bit string with the public 2-universal hash

function from Step 7 of the encryption. 9. Output M=C.sub.K.sup.-1(e). The original CSC decryption needs one single exponentiation and one combined double exponentiation, whereas XTR-CSC decryption requires three exponentiations in the subgroup (and a square-root computation in GF(p) for Step 1). It follows from Remarks 2.4.6 and 2.5.5 that the total computational effort for the latter exponentiations is less than one third of the total effort of the former, assuming the original CSC is implemented using traditional subgroups. If the full multiplicative group is used for the original CSC, then using XTR-CSC instead is even more advantageous (col.33, lines 33-50). Thus, the Qu and Lenstra combination would have been obvious for a person of ordinary skills in the art for three exponentiation operations because this reduces the bandwidth and the computational effort required to generate keys (Lenstra - col.2, lines 20-27 and col.33, lines 33-50).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Qu, et al. (US 6,792,530), and in view of Lenstra, et al. (US 7,076,061).

As per claim 1:

Roy discloses the method for generating a shared key comprising:

providing a first certificate from a first peer to a second peer, the first certificate including a plurality of first parameters, the first peer and second peer being communicated over a network; **(col.2, lines 26-36)**

performing a first exponentiation operation to generate a first public key from the second peer using at least one parameter of the plurality of first parameters and a first private key from the second peer, wherein the first parameters being digital signature standard parameters; **(col.2, lines 38-47 and col.3, lines 57-67)**

providing a second certificate and the first public key from the second peer to the first peer, the second certificate comprising a plurality of second parameters; **(col.9, lines 20-67 and col.17, lines 1-21)**

performing a second exponentiation operation to generate a first shared secret key for the second peer using at least one parameter from the plurality of first parameters; **(col.17, lines 25-45 and col.20, line 1)**

performing a third exponentiation operation to generate a second shared secret key for the first peer using the first public key from the second peer and a private key from the first peer. **(col.17, lines 64-67 and col.20, line 2-8)**

Qu teaches an invention that seeks to provide an efficient ID-based implicit certificate scheme, which provides improved computational speeds over existing schemes (col.2, lines 26-29). Qu teaches reconstructing user A's public key needs only 3 known basis exponentiation operations and 3 multiplication operations. When the signature is valid, CA2, CA3, and user A's public key are implicitly verified (col.18, lines 22-28). Qu further discloses suggests the claimed invention where with the implicit certificate scheme, each party only does three exponentiation operations to get the

shared key while at the same time performing authentication key agreement and implicit public key verification (col.20, line 1-8). Qu did not suggest the advantage of the three exponentiation operations. Thus, Lenstra is combined with Qu.

Lenstra teaches the invention that provides improvements on in key generation and cryptographic applications in public key cryptography, by both reducing: 1) the bit-length of public keys and other messages, thereby reducing the bandwidth requirements of telecommunications devices, such as wireless telephone sets, and 2) the computational effort required to generate keys, to encrypt/decrypt and to generate/verify digital signatures (col.2, lines 20-27). Lenstra discloses the use Algorithm 2.4.4 with n=z and B replaced by xtr(u.sub.1) to compute .kappa.=xtr((g.sub.1).sup.zr). 8. As in [8: Section 5.2], compute the decryption key K by hashing .kappa. to an l-bit string with the public 2-universal hash function from Step 7 of the encryption. 9. Output M=C.sub.K.sup.-1(e). The original CSC decryption needs one single exponentiation and one combined double exponentiation, whereas XTR-CSC decryption requires three exponentiations in the subgroup (and a square-root computation in GF(p) for Step 1). It follows from Remarks 2.4.6 and 2.5.5 that the total computational effort for the latter exponentiations is less than one third of the total effort of the former, assuming the original CSC is implemented using traditional subgroups. If the full multiplicative group is used for the original CSC, then using XTR-CSC instead is even more advantageous (col.33, lines 33-50).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine Qu and Lenstra to teach generating a shared key comprises three exponentiation operations because reducing the bandwidth and the computational effort required to generate keys (Lenstra - col.2, lines 20-27 and col.33, lines 33-50).

As per claim 2: **See Qu on col.3, lines 57-67;** discussing the method according to claim 1

wherein the first certificate is a DSA type certificate.

As per claim 3: **See Qu on col.20, line 1-8 and col.18, lines 22-28;** discussing the method according to claim 2 wherein the first and second parameters comprise a prime number p.sub.dss, a prime number q.sub.dss a generator g.sub.dss and a public key for the first and second peers, respectively.

As per claim 4: **See Qu on col.17, line 1-67 and col.18, lines 22-28;** discussing the method according to claim 3 wherein the first exponentiation operation to generate the first public key is Y.sub.R=g.sub.dss{circumfle- x over ( )}X.sub.R mod p.sub.dss where X.sub.R is a one-time private key from the second peer.

As per claim 5: **See Qu on col.17, line 1-67 and col.18, lines 22-28;** discussing the method according to claim 4 wherein the second exponentiation operation to generate the shared secret key for the second peer is .sub.SSK=Y.sub.Adss{circumflex over ( )}X.sub.R mod p.sub.dss where Y.sub.Adss is a DSS public key from certificate of peer A.

As per claim 6: **See Qu on col.17, line 1-67 and col.18, lines 22-28;** discussing the method according to claim 5 wherein Y.sub.Adss=g.sub.dss{circumflex over ( )}X.sub.Adss mod p.sub.dss where X.sub.Adss is a DSS private key from certificate of peer A.

As per claim 7: **See Qu on col.17, line 1-67 and col.18, lines 22-28;** discussing the method according to claim 5 wherein the third exponentiation operation to generate the shared secret key for the first peer is Y.sub.SSK=YR{circumflex over ( )}X.sub.Adss mod p.sub.dss where X.sub.Adss is a DSS private key from certificate of peer A.

As per claim 8: **See Lenstra on col.2, lines 23-26;** discussing the method according to claim 1 wherein the first and second certificates are sent to the second and first peers, respectively, over a

wireless network.

As per claim 9:

Roy discloses the article of manufacture comprising:

a machine accessible storage medium including data that, when accessed by a machine, causes the machine to perform operations comprising:

providing a first certificate from a first peer to a second peer, the first certificate including a plurality of first parameters; **(col.2, lines 26-36)**

performing a first exponentiation operation to generate a first public key from the second peer using the plurality of first parameters and the first private key from the second peer; **(col.2, lines 38-47 and col.3, lines 57-67)**

providing a second certificate and the first public key from the second peer to the first peer, the second certificate comprising a plurality of second parameters; **(col.9, lines 20-67 and col.17, lines 1-21)**

performing a second exponentiation operation to generate a first shared secret key for the second peer using at least one parameter from the plurality of first parameters; **(col.17, lines 25-45 and col.20, line 1)**

performing a third exponentiation operation to generate a second shared secret key for the first peer using the first public key from the second peer and a private key from the first peer. **(col.17, lines 64-67 and col.20, line 2)**

Qu teaches an invention that seeks to provide an efficient ID-based implicit certificate scheme, which provides improved computational speeds over existing schemes (col.2, lines 26-29). Qu teaches reconstructing user A's public key needs only 3 known basis exponentiation operations and 3

multiplication operations. When the signature is valid, CA2, CA3, and user A's public key are implicitly verified (col.18, lines 22-28). Qu further discloses suggests the claimed invention where with the implicit certificate scheme, each party only does three exponentiation operations to get the shared key while at the same time performing authentication key agreement and implicit public key verification (col.20, line 1-8). Qu did not suggest the advantage of the three exponentiation operations. Thus, Lenstra is combined with Qu.

Lenstra teaches the invention that provides improvements on in key generation and cryptographic applications in public key cryptography, by both reducing: 1) the bit-length of public keys and other messages, thereby reducing the bandwidth requirements of telecommunications devices, such as wireless telephone sets, and 2) the computational effort required to generate keys, to encrypt/decrypt and to generate/verify digital signatures (col.2, lines 20-27). Lenstra discloses the use Algorithm 2.4.4 with n=z and B replaced by xtr(u.sub.1) to compute .kappa.=xtr((g.sub.1).sup.zr). 8. As in [8: Section 5.2], compute the decryption key K by hashing .kappa. to an l-bit string with the public 2-universal hash function from Step 7 of the encryption. 9. Output M=C.sub.K.sup.-1(e). The original CSC decryption needs one single exponentiation and one combined double exponentiation, whereas XTR-CSC decryption requires three exponentiations in the subgroup (and a square-root computation in GF(p) for Step 1). It follows from Remarks 2.4.6 and 2.5.5 that the total computational effort for the latter exponentiations is less than one third of the total effort of the former, assuming the original CSC is implemented using traditional subgroups. If the full multiplicative group is used for the original CSC, then using XTR-CSC instead is even more advantageous (col.33, lines 33-50).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine Qu and Lenstra to teach generating a shared key comprises three exponentiation operations because

reducing the bandwidth and the computational effort required to generate keys (Lenstra - col.2, lines 20-27 and col.33, lines 33-50).

As per claim 10: See Qu on col.9, lines 32-35; discussing the article of manufacture according to claim 9 wherein the first certificate is a DSA type certificate.

As per claim 11: See Qu on col.20, line 1-8 and col.18, lines 22-28; discussing the article of manufacture according to claim 10 wherein the first and second parameters comprise a prime number p.sub.dss, a prime number q.sub.dss, a generator g.sub.dss and a public key for the first and second peers, respectively.

As per claim 12: See Qu on col.20, line 1-8 and col.18, lines 22-28; discussing the article of manufacture according to claim 11 wherein the first exponentiation operation to generate the first public key is Y.sub.R=g.sub.dss{circumflex over ( )}XR mod p.sub.dss where X.sub.R is a one-time private key from the second peer.

As per claim 13: See Qu on col.20, line 1-8 and col.18, lines 22-28; discussing the article of manufacture according to claim 12 wherein the second exponentiation operation to generate the shared secret key for the second peer is Y.sub.SSK=Y.sub.Adss{circumflex over ( )}X.sub.R mod p.sub.dss where Y.sub.Adss is a DSS public key from certificate of peer A.

As per claim 14: See Qu on col.20, line 1-8 and col.18, lines 22-28; discussing the article of manufacture according to claim 13 wherein Y.sub.Adss=g.sub.dss{circumflex over ( )}X.sub.Adss mod p.sub.dss where X.sub.Adss is a DSS private key from certificate of peer A.

As per claim 15: See Qu on col.20, line 1-8 and col.18, lines 22-28; discussing the article of manufacture according to claim 13 wherein the third exponentiation operation to generate the shared secret key for the first peer is Y.sub.SSK=Y.sub.R{circumflex over ( )} X.sub.Adss mod p.sub.dss

where X.sub.Adss is a DSS private key from certificate of peer A.

As per claim 16: See Lenstra on col.2, lines 23-26; discussing the article of manufacture according to claim 9 wherein the first and second certificates are sent to the second and first peers, respectively, over a wireless network.

As per claim 17:

Roy discloses a system comprising:

a processor; and a memory coupled to the processor, the memory containing program code that, when executed by the processor, causes the processor to:

provide a first certificate from a first peer to a second peer, the first certificate including a plurality of first parameters; **(col.2, lines 26-36)**

perform a first exponentiation operation to generate a first public key from the second peer using the plurality of first parameters and the first private key from the second peer; **(col.2, lines 38-47 and col.3, lines 57-67)**

provide a second certificate and the first public key from the second peer to the first peer; the second certificate comprising a plurality of second parameters; **(col.9, lines 20-67 and col.17, lines 1-21)**

perform a second exponentiation operation to generate a first shared secret key for the second peer using at least one parameter from the plurality of first parameters; **(col.17, lines 25-45 and col.20, line 1)**

perform a third exponentiation operation to generate a second shared secret key for the first peer using the first public key from the second peer and a private key from the first peer. **(col.17, lines 64-67 and col.20, line 2)**

Qu teaches an invention that seeks to provide an efficient ID-based implicit certificate scheme, which provides improved computational speeds over existing schemes (col.2, lines 26-29). Qu teaches reconstructing user A's public key needs only 3 known basis exponentiation operations and 3 multiplication operations. When the signature is valid, CA2, CA3, and user A's public key are implicitly verified (col.18, lines 22-28). Qu further discloses suggests the claimed invention where with the implicit certificate scheme, each party only does three exponentiation operations to get the shared key while at the same time performing authentication key agreement and implicit public key verification (col.20, line 1-8). Qu did not suggest the advantage of the three exponentiation operations. Thus, Lenstra is combined with Qu.

Lenstra teaches the invention that provides improvements on in key generation and cryptographic applications in public key cryptography, by both reducing: 1) the bit-length of public keys and other messages, thereby reducing the bandwidth requirements of telecommunications devices, such as wireless telephone sets, and 2) the computational effort required to generate keys, to encrypt/decrypt and to generate/verify digital signatures (col.2, lines 20-27). Lenstra discloses the use Algorithm 2.4.4 with n=z and B replaced by xtr(u.sub.1) to compute .kappa.=xtr((g.sub.1).sup.zr). 8. As in [8: Section 5.2], compute the decryption key K by hashing .kappa. to an l-bit string with the public 2-universal hash function from Step 7 of the encryption. 9. Output M=C.sub.K.sup.-1(e). The original CSC decryption needs one single exponentiation and one combined double exponentiation, whereas XTR-CSC decryption requires three exponentiations in the subgroup (and a square-root computation in GF(p) for Step 1). It follows from Remarks 2.4.6 and 2.5.5 that the total computational effort for the latter exponentiations is less than one third of the total effort of the former, assuming the

original CSC is implemented using traditional subgroups. If the full multiplicative group is used for the original CSC, then using XTR-CSC instead is even more advantageous (col.33, lines 33-50).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine Qu and Lenstra to teach generating a shared key comprises three exponentiation operations because reducing the bandwidth and the computational effort required to generate keys (Lenstra - col.2, lines 20-27 and col.33, lines 33-50).

As per claim 18: See col.3, lines 57-67; discussing the system according to claim 17 wherein the first certificate is a DSA type certificate.

As per claim 19: See Qu on col.20, line 1-8 and col.18, lines 22-28; discussing the system according to claim 18 wherein the first and second parameters comprise a prime number p.sub.dss, a prime number q.sub.dss, a generator g.sub.dss and a public key for the first and second peers, respectively.

As per claim 20: See Qu on col.20, line 1-8 and col.18, lines 22-28; discussing the system according to claim 19 wherein the first exponentiation operation to generate the first public key is Y.sub.R=g.sub.dss{circumfle- x over ( )}X.sub.R mod p.sub.dss where X.sub.R is a one-time private key from the second peer.

As per claim 21: See Qu on col.20, line 1-8 and col.18, lines 22-28; discussing the system according to claim 20 wherein the second exponentiation operation to generate the shared secret key for the second peer is Y.sub.SSK=Y.sub.dss{circumflex over ( )}X.sub.R mod p.sub.dss where Y.sub.Adss is a DSS public key from certificate of peer A.

As per claim 22: See Qu on col.20, line 1-8 and col.18, lines 22-28; discussing the system according to claim 21 wherein Y.sub.Adss=g.sub.dss{circumfl- ex over ( )}X.sub.Adss where

X.sub.Adss is a DSS private key from certificate of peer A.

As per claim 23: See Qu on col.20, line 1-8 and col.18, lines 22-28; discussing the system according to claim 21 wherein the third exponentiation operation to generate the shared secret key for the first peer is Y.sub.SSK=YR{circumflex over ( )}X.sub.Adss mod p.sub.dss where X.sub.Adss is a DSS private key from certificate of peer A.

As per claim 24: See Lenstra on col.2, lines 23-26; discussing the system according to claim 17 wherein the first and second certificates are sent to the second and first peers, respectively, over a wireless network.

As per claim 25:

Roy discloses a method comprising:

receiving a first certificate including a plurality first parameters; **(col.2, lines 26-36)**

performing a first exponentiation operation to generate a first public key using at least one parameter of the plurality of first parameters and a first private key; **(col.2, lines 38-47 and col.3, lines 57-67)**

receiving a second certificate and the first public key, the second certificate including a plurality of second parameters; **(col.9, lines 20-67 and col.17, lines 1-21)**

performing a second exponentiation operation to generate a first shared secret key using at least one parameter from the plurality of first parameters; **(col.17, lines 25-45 and col.20, line 1)**

performing a third exponentiation operation to generate a second shared secret key using the first public key and a private key. **(col.17, lines 64-67 and col.20, line 2)**

Qu teaches an invention that seeks to provide an efficient ID-based implicit certificate scheme, which provides improved computational speeds over existing schemes (col.2, lines 26-29). Qu

teaches reconstructing user A's public key needs only 3 known basis exponentiation operations and 3 multiplication operations. When the signature is valid, CA2, CA3, and user A's public key are implicitly verified (col.18, lines 22-28). Qu further discloses suggests the claimed invention where with the implicit certificate scheme, each party only does three exponentiation operations to get the shared key while at the same time performing authentication key agreement and implicit public key verification (col.20, line 1-8). Qu did not suggest the advantage of the three exponentiation operations. Thus, Lenstra is combined with Qu.

Lenstra teaches the invention that provides improvements on in key generation and cryptographic applications in public key cryptography, by both reducing: 1) the bit-length of public keys and other messages, thereby reducing the bandwidth requirements of telecommunications devices, such as wireless telephone sets, and 2) the computational effort required to generate keys, to encrypt/decrypt and to generate/verify digital signatures (col.2, lines 20-27). Lenstra discloses the use Algorithm 2.4.4 with n=z and B replaced by xtr(u.sub.1) to compute .kappa.=xtr((g.sub.1).sup.zr). 8. As in [8: Section 5.2], compute the decryption key K by hashing .kappa. to an l-bit string with the public 2-universal hash function from Step 7 of the encryption. 9. Output M=C.sub.K.sup.-1(e). The original CSC decryption needs one single exponentiation and one combined double exponentiation, whereas XTR-CSC decryption requires three exponentiations in the subgroup (and a square-root computation in GF(p) for Step 1). It follows from Remarks 2.4.6 and 2.5.5 that the total computational effort for the latter exponentiations is less than one third of the total effort of the former, assuming the original CSC is implemented using traditional subgroups. If the full multiplicative group is used for the original CSC, then using XTR-CSC instead is even more advantageous (col.33, lines 33-50).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine Qu and Lenstra to teach generating a shared key comprises three exponentiation operations because reducing the bandwidth and the computational effort required to generate keys (Lenstra - col.2, lines 20-27 and col.33, lines 33-50).

As per claim 26: **See col.3, lines 57-67;** discussing the method according to claim 25 wherein the first certificate is a DSA type certificate.

As per claim 27: **See Qu on col.20, line 1-8 and col.18, lines 22-28;** discussing the method according to claim 26 wherein the first and second parameters each comprises a prime number p.sub.dss, a prime number q.sub.dss, a generator g.sub.dss and a public key.

As per claim 28: **See Qu on col.20, line 1-8 and col.18, lines 22-28;** discussing the method according to claim 27 wherein the first exponentiation operation to generate the first public key is Y.sub.R=g.sub.dss{circumfle- x over ( )}X.sub.R mod P.sub.dss where X.sub.R is a one-time private key.

As per claim 29: **See Qu on col.20, line 1-8 and col.18, lines 22-28;** discussing the method according to claim 28 wherein the second exponentiation operation to generate the first shared secret key for the second peer is .sub.SSK=Y.sub.Adss {circumflex over ( )}X.sub.R mod p.sub.dss where Y.sub.Adss is a DSS public key.

As per claim 30: **See Qu on col.20, line 1-8 and col.18, lines 22-28;** discussing the method according to claim 29 wherein Y.sub.Adss=g.sub.dss{circumfl- ex over ( )}X.sub.Adss mod p.sub.dss where X.sub.Adss is a DSS private key.

As per claim 31: **See Qu on col.20, line 1-8 and col.18, lines 22-28;** discussing the method according to claim 29 wherein the third exponentiation operation to generate a second shared secret

key is Y.sub.SSK=Y.sub.R{circumflex over ( )}X.sub.Adss mod p.sub.dss where X.sub.Adss is a DSS private key.

As per claim 32: **See Lenstra on col.2, lines 23-26;** discussing the method according to claim 25 wherein the first and second certificates are sent to the second and first peers, respectively, over a wireless network.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 33-35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Qu, et al. (US 6,792,530) and Lenstra, et al. (US 7,076,061), and further in view of Yeager, et al. (US 7,222,187).

As per claim 33: Qu and Lenstra combination teaches generating a shared key comprises three exponentiation operations for reducing the bandwidth and the computational effort required to generate keys (Lenstra - col.2, lines 20-27 and col.33, lines 33-50). However, did not include Bluetooth technology or Bluetooth network.

Yeager discloses Embodiments of a decentralized, distributed trust mechanism are described that may be used in various networking platforms, including, but not limited to, peer-to-peer and other decentralized networking platforms. The mechanism may be used, among other things, to implement trust relationships between and among peers and to implement trust relationships between peers and

content and data (col.2, lines 44-50). Roy discusses the peer-to-peer platform may be independent of specific security approaches where the peer-to-peer platform may provide a comprehensive set of security primitives to support the security solutions used by various peer-to-peer platform services and applications. Embodiments of the peer-to-peer platform may provide one or more security primitives including, but not limited to: A simple crypto library supporting hash functions (e.g. MD5), symmetric encryption algorithms (e.g. RC4), and asymmetric crypto algorithms (e.g., Diffie-Hellman and RSA) (col.58, line 61 – col.57, line 4). Roy further discloses that in order to interact with other peers the peer needs to be connected to some kind of network (wired or wireless) such as, IP, Bluetooth, or Havi, among others (col.27, lines 31-35) and that peer-to-peer platform may be independent of transport protocols (col.33, lines 21-25). For example, the peer-to-peer platform may be implemented on top of TCP/IP, HTTP, Bluetooth, HomePNA and other protocols.

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teaching of the Qu and Lenstra combination with Yeager to teach a Bluetooth network because in order to interact with other peers the peer needs to be connected to some kind of network (wired or wireless) such as Bluetooth (Yeager -col.27, lines 31-35) and peer-to-peer platform may be independent of transport protocols that may be implemented on top Bluetooth (Yeager -col.33, lines 21-25).

As per claim 34: Qu and Lenstra combination teaches generating a shared key comprises three exponentiation operations for reducing the bandwidth and the computational effort required to generate keys (Lenstra - col.2, lines 20-27 and col.33, lines 33-50). However, did not include Bluetooth technology or Bluetooth network.

Yeager discloses Embodiments of a decentralized, distributed trust mechanism are described that may be used in various networking platforms, including, but not limited to, peer-to-peer and other decentralized networking platforms. The mechanism may be used, among other things, to implement trust relationships between and among peers and to implement trust relationships between peers and content and data (col.2, lines 44-50). Roy discusses the peer-to-peer platform may be independent of specific security approaches where the peer-to-peer platform may provide a comprehensive set of security primitives to support the security solutions used by various peer-to-peer platform services and applications. Embodiments of the peer-to-peer platform may provide one or more security primitives including, but not limited to: A simple crypto library supporting hash functions (e.g. MD5), symmetric encryption algorithms (e.g. RC4), and asymmetric crypto algorithms (e.g., Diffie-Hellman and RSA) (col.58, line 61 – col.57, line 4). Roy further discloses that in order to interact with other peers the peer needs to be connected to some kind of network (wired or wireless) such as, IP, Bluetooth, or Havi, among others (col.27, lines 31-35) and that peer-to-peer platform may be independent of transport protocols (col.33, lines 21-25). For example, the peer-to-peer platform may be implemented on top of TCP/IP, HTTP, Bluetooth, HomePNA and other protocols.

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teaching of Roy with Yeager to teach a Bluetooth network because in order to interact with other peers the peer needs to be connected to some kind of network (wired or wireless) such as Bluetooth (col.27, lines 31-35) and peer-to-peer platform may be independent of transport protocols that may be implemented on top Bluetooth (col.33, lines 21-25).

As per claim 35: Qu and Lenstra combination teaches generating a shared key comprises three exponentiation operations for reducing the bandwidth and the computational effort required to

generate keys (Lenstra - col.2, lines 20-27 and col.33, lines 33-50). However, did not include Bluetooth technology or Bluetooth network.

Yeager discloses Embodiments of a decentralized, distributed trust mechanism are described that may be used in various networking platforms, including, but not limited to, peer-to-peer and other decentralized networking platforms. The mechanism may be used, among other things, to implement trust relationships between and among peers and to implement trust relationships between peers and content and data (col.2, lines 44-50). Roy discusses the peer-to-peer platform may be independent of specific security approaches where the peer-to-peer platform may provide a comprehensive set of security primitives to support the security solutions used by various peer-to-peer platform services and applications. Embodiments of the peer-to-peer platform may provide one or more security primitives including, but not limited to: A simple crypto library supporting hash functions (e.g. MD5), symmetric encryption algorithms (e.g. RC4), and asymmetric crypto algorithms (e.g., Diffie-Hellman and RSA) (col.58, line 61 – col.57, line 4). Roy further discloses that in order to interact with other peers the peer needs to be connected to some kind of network (wired or wireless) such as, IP, Bluetooth, or Havi, among others (col.27, lines 31-35) and that peer-to-peer platform may be independent of transport protocols (col.33, lines 21-25). For example, the peer-to-peer platform may be implemented on top of TCP/IP, HTTP, Bluetooth, HomePNA and other protocols.

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teaching of Roy with Yeager to teach a Bluetooth network because in order to interact with other peers the peer needs to be connected to some kind of network (wired or wireless) such as Bluetooth (col.27, lines 31-35) and peer-to-peer platform may be independent of transport protocols that may be implemented on top Bluetooth (col.33, lines 21-25).

Conclusion

5. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Leynna T. Truvan whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/L. T. T./
Examiner, Art Unit 2135
/KimYen Vu/
Supervisory Patent Examiner, Art Unit 2135